Three-Transmit-Antenna Space-Time Codes Based on $SU(3)$

Yindi Jing and Babak Hassibi

***Abstract*—*Fully diverse* constellations, i.e., a set of unitary matrices whose pairwise differences are nonsingular, are useful in multiantenna communications especially in multiantenna differential modulation, since they have good pairwise error properties. Recently, group theoretic ideas, especially *fixed-point-free (fpf)* groups, have been used to design fully diverse constellations of unitary matrices. Here, we give systematic design methods of space-time codes which are appropriate for three-transmit-antenna differential modulation. The structures of the codes are motivated by the special unitary Lie group $SU(3)$. One of the codes, which is called the AB code, has a fast maximum-likelihood (ML) decoding algorithm using complex sphere decoding. Diversity products of the codes can be easily calculated, and simulated performance shows that they are better than group-based codes, especially at high rates and as good as the elaborately designed nongroup code.**

***Index Terms*—Diversity product, Lie group, multiple-antenna system, space-time code.**

I. Introduction

It is well known in theory that multiple antennas can greatly increase the data rate and the reliability of a wireless communication link in a fading environment. In practice, however, one needs to devise effective space-time transmission schemes. This is particularly challenging when the propagation environment is unknown to both the sender and the receiver, which is often the case for mobile applications when the channel changes rapidly.

A differential transmission scheme called *differential unitary space-time modulation* was proposed in [1]–[3], which is well tailored for unknown continuously varying Rayleigh flat-fading channels. The signals transmitted are unitary matrices. In this scheme, the probability of mistaking one signal U_i for another $U_{i'}$, at high SNR, is proved to be inversely proportional to $|\det(U_i - U_{i'})|$. Therefore, the quality of the code is measured by its *diversity product*

$$\zeta_{\mathcal{C}} = \frac{1}{2} \min_{U_i \neq U_{i'} \in \mathcal{C}} |\det(U_i - U_{i'})|^{1/M} \tag{1}$$

where M is the number of transmit antennas, and $\mathcal{C}$ is the set of all possible signals. We therefore say that a code is *fully diverse* if the determinants of the pairwise differences are all nonzero. The design problem is thus the following: "Given the number of transmitter antennas M and the transmission rate R, find a set $\mathcal{C}$ of $L = 2^{MR}$ $M \times M$ unitary matrices, such that its diversity product is as large as possible."

Space-time code design methods for systems with three transmit antennas are rare. Until now, some group-based and nongroup codes have been proposed in [4]. The group-based codes, mainly the G_{mr} codes and the diagonal cyclic group codes, do not give good performances for high rates. The design of the nongroup codes are very difficult, and the decoding of both codes needs exhaustive search. In this paper, we propose design methods for three-transmit-antenna systems. The codes are motivated by the Lie group $SU(3)$. The reasons of analyzing $SU(3)$ are as follows.

The unitary space-time code design problem given above appears to be intractable since both the signal set and the cost function are nonconvex, and the size of the problem can be huge, especially for high data rates. Therefore, in [4]–[6], group structure was introduced on constellation sets to have hope of obtaining a solution. Group structure has the advantages of simplifying the design criterion and easy encoding. In [4], all finite fully diverse constellations, which form a group, are classified. (For the definition and more of fpf groups, see [6].) In addition, in [6], it is proved that the only fpf infinite Lie groups are $U(1)$ (the group of unit-modulus scalars) and $SU(2)$ (the group of unit-determinant 2×2 unitary matrices). However, no good constellations are obtained for very high rates from fpf finite groups, and constellations based on $U(1)$ and $SU(2)$ are constrained to one and two-transmit-antenna systems. (Codes constructed based on higher dimensional representations of $SU(2)$ can be found in [7].) As mentioned in [8], to get high-rate constellations that work for systems with more than two transmit antennas, we relax the fpf condition by considering Lie groups of rank 2. (The *rank* of a Lie group equals the maximum number of commuting basis elements of its Lie algebra and it can be shown that fpf groups have rank 1.) There are three of them: the Lie group of unit-determinant 3×3 unitary matrices $SU(3)$, the Lie group of 4×4 unitary, symplectic matrices $Sp(2)$, and one exceptional Lie group $\mathcal{G}_2$. Constellations based on $Sp(2)$, which can be regarded as an extension of the Alamouti's scheme [9], are designed in [8], and simulation results show that they have good performance. In this work, we analyze $SU(3)$.

Based on the structure of matrices in $SU(3)$, we propose two methods to design constellations of 3×3 unitary matrices. One

Manuscript received May 14, 2004; revised November 20, 2004. This work was supported by the Air Force Office for Scientific Research for MURI "Mathematical Infrastructure for Robust Virtual Engineering," URI "Protecting Infrastructures from Themselves," and Caltech's Lee Center for Advanced Networking. This work was supported in part by the National Science Foundation under Grant CCR-0133818, by the office of Naval Research under Grant N00014-02-1-0578, and by Caltech's Lee Center for Advanced Networking. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Carlos H. Muravchik.

The authors are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: yindi@systems.caltech.edu; hassibi@systems.caltech.edu).

Digital Object Identifier 10.1109/TSP.2005.855092

of the method gives codes that are subsets of $SU(3)$. The other codes are derived from $SU(3)$ codes by a simple modification, which are called AB codes. The codes also have the structure of products of group representations discussed in [4, Section 8]. Simple formulas are derived by which diversity products of the codes can be calculated in a fast way. Necessary conditions for full diversity of the codes are proved. Our conjecture is that they are also sufficient conditions. Simulation results show that the codes have better performance than group-based codes [4], especially at high rates, and are as good as the elaborately designed nongroup code [4]. Another exceptional feature of AB codes is that they have a fast maximum-likelihood decoding algorithm based on complex sphere decoding.

The paper is organized as follows. In Section I-A, we talk briefly about the multiple-antenna system model we are using and differential unitary space-time modulation. A brief introduction and discussion on the Lie group $SU(3)$, emphasizing the parametrization method of $SU(3)$ we have proved, is given in Section II. In Section III, $SU(3)$ codes are proposed, and their diversity products are analyzed. In Section IV, we propose AB codes whose structure is obtained by making a slight modification on $SU(3)$ codes. A fast decoding algorithm of AB codes using complex sphere decoding is shown in Section V. Simulation results, including comparisons with other existing constellations such as group-based codes and a nongroups code, are presented in Section VI. Section VII concludes the paper. Some of the proofs of the theorems and lemmas in this paper are relegated to the Appendixes.

A. *Differential Unitary Space-Time Modulation*

Before bringing in the design of space-time codes, we first present a brief introduction to multiple-antenna systems and the differential unitary space-time signaling scheme. This follows [1]–[3].

Consider a wireless communication system with M transmit antennas and N receive antennas. We use a block-fading channel with coherence interval T (for more on this model, see [10], [11]). The system equation of the τth block can be written as

$$X_\tau = \sqrt{\frac{\rho T}{M}} S_\tau H_\tau + W_\tau.$$

Here, S_τ denotes the $T \times M$ transmit signal matrix with its (t, m)th entry s_{tm}, which is the signal sent by the mth transmit antenna at time t. H_τ is the $M \times N$ propagation matrix that remains constant during the coherence interval, and its (m, n)th entry h_{mn} is the propagation coefficient between the mth transmit antenna and the nth receive antenna. The h_{mn}s have a zero-mean unit-variance circularly symmetric complex Gaussian distribution $\mathcal{CN}(0, 1)$ and are independent of each other. We assume that the channel information is unknown to both the transmitter and the receiver. W_τ is the $T \times N$ noise matrix with its (t, n)th entry w_{tn}, which is the noise at the nth receive antenna at time t. The w_{tn}s are iid with $\mathcal{CN}(0, 1)$ distribution. X_τ is the $T \times N$ received signal matrix with its (t, n)th entry x_{tn}, which is the received value by the nth receive antenna at time t. We impose an extra power constraint on the transmit signal

$$\frac{1}{M} \sum_{m=1}^{M} \exp |s_{tm}|^2 = \frac{1}{T}, \quad t = 1, 2, \ldots, T$$

which means that the transmit signal s_{tm} has average expected power (over the M transmit antennas) $1/T$ at each channel use. Therefore, ρ represents the expected SNR at each receive antenna.

One way to communicate with unknown channel information is to use multiple-antenna differential unitary space-time modulation (USTM), which can be seen as a natural extension of the standard differential phase shift keying (DPSK) that is commonly used in signal-antenna unknown-channel systems. In differential USTM, the channel is used in blocks of M transmissions, that is, $T = M$, which implies that the transmit signal S_τ is an $M \times M$ unitary matrix. At the τth block, the transmit matrix equals the product of the previously transmit matrix and a unitary data matrix U_{z_τ}, $z_\tau \in \{0, \ldots, L-1\}$ taken from our signal set $\mathcal{C}$. In other words

$$S_\tau = U_{z_\tau} S_{\tau-1}$$

with $S_0 = I_M$. Having U_{z_τ} unitary assures that the transmit signal will not vanish or blow up to infinity. Since the channel is used M times, the corresponding transmission rate is $R = (1/M) \log_2 L$, where L is the cardinality of the code. If we further assume that the propagation environment keeps approximately constant for $2M$ consecutive channel uses, that is, $H_\tau \approx H_{\tau-1}$, then from the system equations for the τth and the $(\tau - 1)$th blocks, the following fundamental differential receiver equations are obtained [12]:

$$X_\tau = U_{z_\tau} X_{\tau-1} + W'_\tau \tag{2}$$

where

$$W'_\tau = W_\tau - U_{z_\tau} W_{\tau-1}. \tag{3}$$

We can see that the channel matrix H does not appear in (2). This implies that as long as the channel is approximately constant for $2M$ channel uses, differential transmission permits decoding without knowing the channel information.

Since U_{z_τ} is unitary, the additive noise term in (3) is statistically independent of U_{z_τ} and has independent complex Gaussian entries. Therefore, the ML decoding of z_τ can be written as[1]

$$\hat{z}_\tau = \arg \min_{l=0,\ldots,L-1} \|X_\tau - U_l X_{\tau-1}\|_F^2 \tag{4}$$

where $\|\cdot\|_F$ indicates the Frobenius norm. It is shown in [1] and [3] that, at high SNR, the pairwise error probability Pe (of transmitting U_l and erroneously decoding $U_{l'}$) has the upper bound

$$Pe \leq \left(\frac{8}{\rho}\right)^{MN} \frac{1}{|\det(U_l - U_{l'})|^{2N}}$$

[1]Here, in decoding U_{z_τ}, only the last two blocks are considered, as in [1]–[3].

which is inversely proportional to the absolute value of the determinant of the pairwise difference to the power of $2N$. Therefore, most design schemes [1], [3]–[5] have focused on finding a constellation $\mathcal{C} = \{U_0, \ldots, U_L\}$ of $L = 2^{MR}$ unitary $M \times M$ matrices that maximizes $\zeta_{\mathcal{C}}$ defined in (1). In general, the number of matrices in $\mathcal{C}$ can be quite large. This huge number of signals calls into question the feasibility of computing $\zeta_{\mathcal{C}}$ and rules out the possibility of decoding via an exhaustive search. To design constellations that are huge, effective, and yet still simple so that they can be decoded in real time, some structure should be imposed on the signal set. Group structure was proposed and used in [4]–[6] and [8], from which good performance can be obtained. In this paper, we analyze the Lie group $SU(3)$ and propose codes that lend themselves to linear-algebraic decoding by using sphere decoding.

II. Parametrization of $SU(3)$

Definition 1: [13] $SU(n)$ is the group of complex $n \times n$ matrices obeying $U^*U = UU^* = I_n$ and $\det U = 1$, where U^* indicates the conjugate transpose of U.

From the definition, $SU(n)$ is the group of complex $n \times n$ unitary matrices with determinant 1. It is called the special unitary group. It is also known that $SU(n)$ is a compact, simply-connected Lie group of dimension $n^2 - 1$ and rank $n - 1$. Since we are most interested in the case of rank 2, here, we focus on $SU(3)$, which has dimension 8. The following theorem on the parametrization of $SU(3)$ is proved.

Theorem 1 (Parametrization of $SU(3)$): Any matrix U belongs to $SU(3)$ if and only if it can be written as

$$U = \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi \end{bmatrix} \begin{bmatrix} a & 0 & -\sqrt{1-|a|^2} \\ 0 & 1 & 0 \\ \sqrt{1-|a|^2} & 0 & \bar{a} \end{bmatrix} \times \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Psi \end{bmatrix} \quad (5)$$

where $\mathbf{0}_{mn}$ denotes the $m \times n$ matrix with all zero entries, $\Phi, \Psi \in SU(2)$, and a is a complex number with $|a| < 1$. □

Proof: See Appendix A.

This theorem indicates that any matrix in $SU(3)$ can be written as a product of three 3×3 unitary matrices that are basically $SU(2)$. (They are actually reducible 3×3 unitary representations of $SU(2)$ by adding an identity block.) Now, let us look at the number of degrees of freedom in U. Since $\Phi, \Psi \in SU(2)$, there are six degrees of freedom in them. Together with the 2 degrees of freedom in a, the dimension of U is 8, which is exactly the same as that of $SU(3)$. Based on (5), we can parameterize matrices in $SU(3)$ by entries of Φ, Ψ, and a, that is, any matrix in $SU(3)$ can be identified with a three-tuple (Φ, Ψ, a). From (5), we can also see that all the three matrices can be regarded as block-diagonal with a unit element. The first and third matrices have the unit element at the (1,1) entry, and the second matrix has the unit element at the (2,2) entry. To get a more symmetric parametrization method, we prove the following corollary.

Corollary 1: Any matrix U belongs to $SU(3)$ if and only if it can be written as

$$U = \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi \end{bmatrix} \begin{bmatrix} \alpha e^{j\omega} & 0 & \sqrt{1-|\alpha|^2}e^{j\beta} \\ 0 & 1 & 0 \\ -\sqrt{1-|\alpha|^2}e^{-j\beta} & 0 & \alpha e^{-j\omega} \end{bmatrix} \times \begin{bmatrix} \Psi & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{bmatrix} \quad (6)$$

where $\Phi, \Psi \in SU(2)$, and $\alpha \in [0,1]$ are real. ω and β are arbitrary angles.

Proof: First, it is easy to prove that any matrix with structure in (6) is in $SU(3)$ by checking the unitary and determinant conditions. What is left to prove is that any matrix in $SU(3)$ can be written as the formula in (6).

For any $U \in SU(3)$, define $U' = U \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. It is easy to check that U' is also in $SU(3)$. Therefore, from Theorem 1, there exist matrices $\Phi', \Psi'' \in SU(2)$ and a complex scalar a such that

$$U' = \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi' \end{bmatrix} \begin{bmatrix} a & 0 & -\sqrt{1-|a|^2} \\ 0 & 1 & 0 \\ \sqrt{1-|a|^2} & 0 & \bar{a} \end{bmatrix} \times \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Psi'' \end{bmatrix}.$$

Denote $\Psi'' = \begin{bmatrix} \psi'_{11} & \psi'_{12} \\ -\bar{\psi}'_{12} & \bar{\psi}'_{11} \end{bmatrix}$, where $|\psi'_{11}|^2 + |\psi'_{12}|^2 = 1$. Note that

$$\begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Psi'' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Psi' & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

where $\Psi' = \begin{bmatrix} \bar{\psi}'_{11} & \bar{\psi}'_{12} \\ -\psi'_{12} & \psi'_{11} \end{bmatrix}$ (it is easy to see that $\Psi' \in SU(2)$). Therefore

$$\begin{aligned} U' &= \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi' \end{bmatrix} \begin{bmatrix} a & 0 & -\sqrt{1-|a|^2} \\ 0 & 1 & 0 \\ \sqrt{1-|a|^2} & 0 & \bar{a} \end{bmatrix} \\ &\quad \times \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} \Psi' & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi' \end{bmatrix} \begin{bmatrix} \sqrt{1-|a|^2} & 0 & a \\ 0 & 1 & 0 \\ -\bar{a} & 0 & \sqrt{1-|a|^2} \end{bmatrix} \\ &\quad \times \begin{bmatrix} \Psi' & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{aligned}$$

and

$$U = \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & \Phi' \end{bmatrix} \begin{bmatrix} \sqrt{1-|a|^2} & 0 & a \\ 0 & 1 & 0 \\ -\bar{a} & 0 & \sqrt{1-|a|^2} \end{bmatrix} \times \begin{bmatrix} \Psi' & \mathbf{0}_{21} \\ \mathbf{0}_{12} & 1 \end{bmatrix}.$$

It is easy to check that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{j\omega} & 0 \\ 0 & 0 & e^{-j\omega} \end{bmatrix} \begin{bmatrix} \sqrt{1-|a|^2} & 0 & a \\ 0 & 1 & 0 \\ -\bar{a} & 0 & \sqrt{1-|a|^2} \end{bmatrix} \times \begin{bmatrix} e^{j\omega} & 0 & 0 \\ 0 & e^{-j\omega} & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \sqrt{1-|a|^2}e^{j\omega} & 0 & a \\ 0 & 1 & 0 \\ -\bar{a} & 0 & \sqrt{1-|a|^2}e^{-j\omega} \end{bmatrix}$$

for any angle ω. Define

$$\Phi = \Phi' \begin{bmatrix} e^{-j\omega} & 0 \\ 0 & e^{j\omega} \end{bmatrix} \text{ and } \Psi = \begin{bmatrix} e^{-j\omega} & 0 \\ 0 & e^{j\omega} \end{bmatrix} \Psi'.$$

It is easy to check that $\Phi, \Psi \in SU(2)$. Equation (6) is obtained by letting $\alpha = \sqrt{1-|a|^2}$ and $\beta = \angle a$. □

The parameter ω does not add a degree of freedom, as can be seen in the proof of the corollary. However, we will see later that it is important to our code design. From (6), any matrix in $SU(3)$ can be written as a product of three basically $SU(2)$ matrices. The first matrix is a representation of an $SU(2)$ matrix with an identity block at the (1,1) entry. The second matrix is a representation of an $SU(2)$ matrix with an identity block at the (2,2) entry, and the third matrix is a representation of an $SU(2)$ matrix with an identity block at the (3,3) entry.

III. $SU(3)$ Code Design

To get finite constellations of unitary matrices from the infinite Lie group $SU(3)$, we need to sample the parameters appropriately. We first sample Φ and Ψ. Alamouti's orthogonal design

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}, \quad |a|^2 + |b|^2 = 1$$

is a faithful representation of $SU(2)$. To get a finite set, a and b must belong to finite sets. As is well known, the PSK signal is a very good and simple modulation. Therefore, Φ and Ψ are chosen as follows:[2]

$$\Phi = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi j(p/P)} & e^{2\pi j(q/Q)} \\ -e^{-2\pi j(q/Q)} & e^{-2\pi j(p/P)} \end{bmatrix}$$
$$\text{and } \Psi = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{2\pi j(r/R)} & e^{2\pi j(s/S)} \\ -e^{-2\pi j(s/S)} & e^{-2\pi j(r/R)} \end{bmatrix}$$

where P, Q, R, and S are positive integers.

Since the group is not fpf, we cannot use all the 8 degrees of freedom to get fully diverse codes. To simplify the structure, we choose $\alpha = 1$, by which the middle matrix in (6) is a diagonal matrix. In addition, we want to obtain fully diverse subsets. Therefore, the angle ω should depend on Φ and Ψ, or equivalently, it is a function of p, q, r, and s. To see this, we assume that ω is independent of Φ. Therefore, the determinant of $U_1(\Phi_1, \Psi, 1, \omega) - U_2(\Phi_2, \Psi, 1, \omega)$ is zero since the first matrix in (6) has a unit block at its (1,1) entry. It is the same for the third matrix in (6). Therefore, we let $\omega = 2\pi(p/P) - (q/Q) + (r/R) + (s/S)$. The reason for this will be illuminated later. Define

$$\theta_{p,q} = 2\pi\left(\frac{p}{P} - \frac{q}{Q}\right) \text{ and } \xi_{r,s} = 2\pi\left(\frac{r}{R} + \frac{s}{S}\right). \quad (7)$$

Equation (6) becomes

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q/Q)} \\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p/P)} \end{bmatrix} \times \text{diag}\left\{e^{\theta_{p,q}}, 1, e^{-\theta_{p,q}}\right\} \text{diag}\left\{e^{\xi_{r,s}}, 1, e^{-\xi_{r,s}}\right\} \times \begin{bmatrix} \frac{1}{\sqrt{2}}e^{2\pi j(r/R)} & \frac{1}{\sqrt{2}}e^{2\pi j(s/S)} & 0 \\ -\frac{1}{\sqrt{2}}e^{-2\pi j(s/S)} & \frac{1}{\sqrt{2}}e^{-2\pi j(r/R)} & 0 \\ 0 & 0 & 1 \end{bmatrix} = A^{(1)}_{(p,q)} B^{(1)}_{(r,s)}$$

where we have defined

$$A^{(1)}_{(p,q)} = \begin{bmatrix} e^{j\theta_{p,q}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q/Q)}e^{-j\theta_{p,q}} \\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p/P)}e^{-j\theta_{p,q}} \end{bmatrix}$$

and

$$B^{(1)}_{(r,s)} = \begin{bmatrix} \frac{1}{\sqrt{2}}e^{2\pi j(r/R)}e^{j\xi_{r,s}} & \frac{1}{\sqrt{2}}e^{2\pi j(s/S)}e^{j\xi_{r,s}} & 0 \\ -\frac{1}{\sqrt{2}}e^{-2\pi j(s/S)} & \frac{1}{\sqrt{2}}e^{-2\pi j(r/R)} & 0 \\ 0 & 0 & e^{-j\xi_{r,s}} \end{bmatrix}. \quad (8)$$

The following codes are obtained:

$$\mathcal{C}^{(1)}_{(P,Q,R,S)} = \Big\{ A^{(1)}_{(p,q)} B^{(1)}_{(r,s)} \,|\, p \in [0,P), q \in [0,Q), r \in [0,R), s \in [0,S) \Big\}. \quad (9)$$

The set is a subset of $SU(3)$. We call it an $SU(3)$ code. There are all together $PQRS$ elements in the code. Since the channel is used in blocks of three transmissions, the rate of the code is

$$R = \frac{1}{3}\log_2(PQRS). \quad (10)$$

Theorem 2 (Calculation of Diversity Product): Define

$$\begin{aligned} x &= e^{2\pi j((p_1-p_2)/2P - (q_1-q_2)/2Q)} \times \cos 2\pi\left(\frac{p_1-p_2}{2P} + \frac{q_1-q_2}{2Q}\right) \\ w &= e^{2\pi j(-(r_1-r_2)/2R - (s_1-s_2)/2S)} \times \cos 2\pi\left(\frac{r_1-r_2}{2R} - \frac{s_1-s_2}{2S}\right). \end{aligned} \quad (11)$$

For $U_1(p_1, q_1, r_1, s_1), U_2(p_2, q_2, r_2, s_2) \in \mathcal{C}^{(1)}_{(P,Q,R,S)}$

$$\det(U_1 - U_2) = 2j\mathcal{I}m[(1-\bar{\Theta}x)(1-\Theta w)] \quad (12)$$

where

$$\Theta = e^{-2\pi j((p_1-p_2)/P - (q_1-q_2)/Q + (r_1-r_2)/R + (s_1-s_2)/S)}.$$

[2]PSK symbols have been analyzed in [14], where it is shown that having a full parametrization of $SU(2)$, that is, parameterizing a and b fully (both the norms and the arguments) gives about a 1–2 dB improvement but with a much more complicated decoding. In our paper, to make our main idea clear, we choose a and b as simple PSK signals.

$\mathcal{I}m[c]$ indicates the imaginary part of the complex scalar c. $\bar{\Theta}$ indicates the conjugate of the complex scalar Θ.

Proof: See Appendix B. □

Therefore, the diversity product of the code is

$$\zeta_{\mathcal{C}^{(1)}}(P,Q,R,S) = \frac{1}{2} \min_{\substack{\delta_p\in(-P,P),\delta_q\in(-Q,Q),\\ \delta_r\in(-R,R),\delta_s\in(-S,S)\\ (\delta_p,\delta_q,\delta_r,\delta_s)\neq(0,0,0,0)}} |2\mathcal{I}m[(1-\bar{\Theta}x)(1-\Theta w)]|^{1/3} \quad (13)$$

where we have defined $\delta_p = p_1 - p_2$, $\delta_q = q_1 - q_2$, $\delta_r = r_1 - r_2$, and $\delta_s = s_1 - s_2$. In general, to obtain diversity product, determinants of $(1/2)L(L-1) = (1/2)(L^2 - L)$ difference matrices, which is quadratic in L, need to be calculated. However, from Theorem 2, x, w, and Θ only depend on the differences δ_p, δ_q, δ_r, and δ_s instead of p_1, p_2, q_1, q_2, r_1, r_2, s_1, and s_2. That is, $\det(U_1 - U_2)$ can be written as $\Delta(\delta_p,\delta_q,\delta_r,\delta_s)$, which is a function of δ_p, δ_q, δ_r, and δ_s. Since δ_p, δ_q, δ_r, and δ_s can take on $2P-1, 2Q-1, 2R-1$, and $2S-1$ possible values, respectively, to get diversity products, we need to calculate determinants of $(2P-1)(2Q-1)(2R-1)(2S-1)-1 < 16PQRS = 16L$ difference matrices, which is linear in L. Actually, instead of $16L$, less than $8L$ calculations is enough. Note that

$$\begin{aligned}|\Delta(\delta_p,\delta_q,\delta_r,\delta_s)| &= |2\mathcal{I}m[(1-\bar{\Theta}x)(1-\Theta w)]|^{1/3}\\ &= |2\mathcal{I}m[(1-\Theta\bar{x})(1-\overline{\Theta w})]|^{1/3}\\ &= |\Delta(-\delta_p,-\delta_q,-\delta_r,-\delta_s)|.\end{aligned}$$

Therefore, calculation of only half of the determinants is needed. The computational complexity for the diversity product is greatly reduced, especially for codes of high rates, that is, when L is large.

From the symmetry of δ_p, δ_q, δ_r, and δ_s in (13), it is easy to prove that $\zeta_{\mathcal{C}^{(1)}}(P,Q,R,S) = \zeta_{\mathcal{C}^{(1)}}(Q,P,R,S) = \zeta_{\mathcal{C}^{(1)}}(P,Q,S,R) = \zeta_{\mathcal{C}^{(1)}}(R,S,P,Q)$, which indicates that changing the positions of P and Q, R and S, or (P,Q) and (R,S) does not effect the diversity product. Generally, however, $\zeta_{\mathcal{C}^{(1)}}(P,Q,R,S) \neq \zeta_{\mathcal{C}^{(1)}}(P,R,Q,S)$.

Theorem 3 (Necessary Condition for Fully Diverse): A necessary condition for code $\mathcal{C}^{(1)}_{(P,Q,R,S)}$ to be fully diverse is that every pair taken from the four integers $\{P,Q,R,S\}$ is relatively prime, and none of them is even.

Proof: See Appendix C. □

We are not able to give a sufficient condition for full diversity of $SU(3)$ codes. Based on the diversity product given in (13) and simulations, we have the following conjecture.

Conjecture 1 (Sufficient Condition for Full Diversity): The condition that every pair of the four integers $\{P,Q,R,S\}$ is relatively prime and none of them is even is sufficient for code $\mathcal{C}^{(1)}_{(P,Q,R,S)}$ to be fully diverse.

IV. AB Code Design

Note from (8) that the $e^{-j\theta_{p,q}}$ in the last column of $A^{(1)}_{p,q}$ and the $e^{j\xi_{r,s}}$ in the first row of $B^{(1)}_{p,q}$ are used to make the matrices determinant 1. However, in differential unitary space-time code design, we only need the signal matrix to be unitary. Therefore, we can further simplify the structure by abandoning the restriction that both the matrices have unit determinant. Define

$$A^{(2)}_{(p,q)} = \begin{bmatrix} e^{j\theta'_{p,q}} & 0 & 0\\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q/Q)}\\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p/P)}\end{bmatrix}$$
$$B^{(2)}_{(r,s)} = \begin{bmatrix} \frac{1}{\sqrt{2}}e^{2\pi j(r/R)} & \frac{1}{\sqrt{2}}e^{2\pi j(s/S)} & 0\\ -\frac{1}{\sqrt{2}}e^{-2\pi j(s/S)} & \frac{1}{\sqrt{2}}e^{-2\pi j(r/R)} & 0\\ 0 & 0 & e^{-j\xi'_{r,s}}\end{bmatrix} \quad (14)$$

and[3]

$$\theta'_{p,q} = 2\pi\left(\pm\frac{p}{P}\pm\frac{q}{Q}\right) \quad \xi'_{r,s} = 2\pi\left(\pm\frac{r}{R}\pm\frac{s}{S}\right). \quad (15)$$

Theorem 4: The set $\left\{A^{(2)}_{(p,q)}, p\in[0,P), q\in[0,Q)\right\}$ is fully diverse if and only if $\gcd(P,Q) = 1$. The set $\left\{B^{(2)}_{(r,s)}, r\in[0,R), s\in[0,S)\right\}$ is fully diverse if and only if $\gcd(R,S) = 1$.

Proof: We first prove that the set

$$\left\{A^{(2)}_{(p,q)}, p\in[0,P), q\in[0,Q)\right\}$$

is fully diverse if and only if P and Q are relatively prime. For any two different matrices $A^{(2)}_{(p_1,q_1)}$ and $A^{(2)}_{(p_2,q_2)}$ in the set

$$A^{(2)}_{(p_1,q_1)} = \begin{bmatrix} e^{j\theta_1} & 0 & 0\\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p_1/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_1/Q)}\\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q_1/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_1/P)}\end{bmatrix}$$
$$A^{(2)}_{(p_2,q_2)} = \begin{bmatrix} e^{j\theta_2} & 0 & 0\\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p_2/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_2/Q)}\\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q_2/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_2/P)}\end{bmatrix}$$

where $\theta_1 = 2\pi(\pm p_1/P \pm q_1/Q)$, $\theta_2 = 2\pi(\pm p_2/P \pm q_2/Q)$, we have the equation at the bottom of the page. The second factor equals zero if and only if $e^{2\pi j(p_1/P)} = e^{2\pi j(p_2/P)}$ and $e^{2\pi j(q_1/Q)} = e^{2\pi j(q_2/Q)}$. Since $p_1, p_2 \in [0,P)$ and $q_1, q_2 \in [0,Q)$, this is equivalent to $(p_1,q_1) = (p_2,q_2)$, which cannot be true since the two matrices are different. Therefore, the determinant equals zero if and only if $e^{j\theta_1} = e^{j\theta_2}$.

[3]There are actually 16 possibilities in (15). Different codes are obtained by different choices of signs. Two of them are used in this paper.

$$\begin{aligned}\det\left(A^{(2)}_{(p_1,q_1)} - A^{(2)}_{(p_2,q_2)}\right) &= \left(e^{j\theta_1} - e^{j\theta_2}\right)\det\begin{bmatrix} \frac{1}{\sqrt{2}}e^{2\pi j(p_1/P)} - \frac{1}{\sqrt{2}}e^{2\pi j(p_2/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_1/Q)} - \frac{1}{\sqrt{2}}e^{2\pi j(q_2/Q)}\\ -\frac{1}{\sqrt{2}}e^{-2\pi j(q_1/Q)} + \frac{1}{\sqrt{2}}e^{-2\pi j(q_2/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_1/P)} - \frac{1}{\sqrt{2}}e^{-2\pi j(p_2/P)}\end{bmatrix}\\ &= \frac{1}{2}\left(e^{j\theta_1} - e^{j\theta_2}\right)\left(\left|e^{2\pi j(p_1/P)} - e^{2\pi j(p_2/P)}\right|^2 + \left|e^{2\pi j(q_1/Q)} - e^{2\pi j(q_2/Q)}\right|^2\right).\end{aligned}$$

Now, assume that $\gcd(P,Q)=G>1$, that is, P and Q are not relatively prime. When $p_1-p_2=P/G$ and $q_1-q_2=-Q/G$ (since G divides both P and Q, this is achievable), we have

$$\begin{aligned}\theta_1-\theta_2 &= 2\pi\left(\pm\frac{p_1-p_2}{P}\pm\frac{q_1-q_2}{Q}\right)\\ &= 2\pi\left(\pm\frac{1}{G}\pm\left(-\frac{1}{G}\right)\right)=0\end{aligned}$$

which means that $e^{j\theta_1}=e^{j\theta_2}$. Therefore, the set $\left\{A^{(2)}_{(p,q)}, p\in[0,P), q\in[0,Q)\right\}$ is not fully diverse.

Now, assume that $\gcd(P,Q)=1$. If $e^{j\theta_1}=e^{j\theta_2}$, $\theta_1-\theta_2=2k\pi$ for some integer k, which means that $\pm(p_1-p_2)/P\pm(q_1-q_2)/Q=k$. Therefore, $(p_1-p_2)/P=\pm kQ\mp(q_1-q_2)/Q$. Since $\gcd(P,Q)=1$, $P|(p_1-p_2)$. However, we know that $p_1-p_2\in(-P+1,P-1)$. The only possibility is that $p_1-p_2=0$. Therefore, $(q_1-q_2)/Q=\pm k$. From $q_1-q_2\in(-Q+1,Q-1)$, $q_1-q_2=0$, and $k=0$. We get $(p_1,q_1)=(p_2,q_2)$, which is a contradiction since the two matrices are different. Therefore, $e^{j\theta_1}\neq e^{j\theta_2}$. So, $\det\left(A^{(2)}_{(p_1,q_1)}-A^{(2)}_{(p_2,q_2)}\right)\neq 0$. Therefore, $\gcd(P,Q)=1$ is a sufficient condition for the set to be fully diverse.

By similar argument, we can prove that the set $\left\{B^{(2)}_{(r,s)}, r\in[0,R), s\in[0,S)\right\}$ is fully diverse if and only if R and S are relatively prime. □

The following codes with a simpler structure are obtained.

$$\mathcal{C}^{(2)}_{(P,Q,R,S)}=\left\{A^{(2)}_{(p,q)}B^{(2)}_{(r,s)}\,|p\in[0,P), q\in[0,Q)\right. \\ \left. r\in[0,R), s\in[0,S)\right\}. \quad (16)$$

They are no longer subsets of the Lie group $SU(3)$ since the determinant of the matrix is now $e^{j(\theta'-\xi')}$, which is not 1 in general. However, matrices in the codes are still unitary. Since any matrix in the code is a product of two unitary matrices (they are no longer representations of $SU(2)$ because their determinants are no longer 1), we call it an AB code. Simulations show that AB codes have the same and sometimes slightly better diversity products than $SU(3)$ codes given in (9), which is not surprising since we now get rid of the constraint of the unit determinant. In Section V, we will see that the handy structure of AB codes results in a fast ML decoding algorithm. The code has the same rate as the $SU(3)$ code. It is easy to see that any matrix U in the two codes can be identified by the four-tuple (p,q,r,s).

Theorem 5 (Calculation of Diversity Product): For any two matrices $U_1(p_1,q_1,r_1,s_1)$ and $U_2(p_2,q_2,r_2,s_2)$ in $\mathcal{C}^{(2)}_{(P,Q,R,S)}$

$$\det(U_1-U_2)=2je^{j\theta'_1}e^{-j\xi'_2}\bar{\Theta}_1\bar{\Theta}_2\mathcal{I}m \\ [(\Theta_1-\bar{\Theta}_1 w)(\bar{\Theta}_2-\Theta_2 x)] \quad (17)$$

where $\Theta_1=e^{2\pi j(\pm(p_1-p_2)/2P\pm(q_1-q_2)/2Q)}$, and $\Theta_2=e^{2\pi j(\pm(r_1-r_2)/2R\pm((s_1-s_2)/2S)}$.

Proof: See Appendix D. □

The diversity product of the AB code is thus (18), shown at the bottom of the page.

Similar to the argument in the previous section, less than $8L$ calculations of the determinants of difference matrices are enough to obtain the diversity product. AB codes also have the symmetry that $\zeta_{\mathcal{C}^{(2)}}(P,Q,R,S)=\zeta_{\mathcal{C}^{(2)}}(Q,P,R,S)=\zeta_{\mathcal{C}^{(2)}}(P,Q,S,R)=\zeta_{\mathcal{C}^{(2)}}(R,S,P,Q)$. Generally, however, $\zeta_{\mathcal{C}^{(2)}}(P,Q,R,S)\neq\zeta_{\mathcal{C}^{(2)}}(P,R,Q,S)$.

As mentioned before, for AB codes, choices for the angles θ' and ξ' are not unique. Based on (15), there are actually 16 possibilities. In Table II, diversity products of AB codes with two of them $\theta'=2\pi(-p/P+q/Q)$, $\xi'=2\pi(-r/R-s/S)$ and $\theta'=2\pi(p/P-q/Q)$, $\xi'=2\pi(-r/R-s/S)$ are given. We call the two codes the type I AB code and the type II AB code, respectively.

Now, let us compare diversity products of some $SU(3)$ codes, as given in Table I, and AB codes, as given in Table II, with other existing 3×3 designs, which are some group-based codes and

TABLE I
DIVERSITY PRODUCTS OF $SU(3)$ CODES

(P,Q,R,S)	Rate	$\frac{1}{2}\min\lvert\det(U_i-U_j)\rvert^{1/3}$
$(5,7,3,1)$	2.2381	0.2133
$(5,7,9,1)$	2.7664	0.1714
$(7,9,11,1)$	3.1456	0.0961
$(3,7,5,11)$	3.3912	0.0803
$(5,9,7,11)$	3.9195	0.0510
$(7,11,9,13)$	4.3791	0.0316

TABLE II
DIVERSITY PRODUCTS OF AB CODES

(P,Q,R,S)	Rate	Type	$\frac{1}{2}\min\lvert\det(U_i-U_j)\rvert^{1/3}$
$(1,3,4,5)$	1.9690	I	0.2977
$(4,5,3,7)$	2.9045	I	0.1413
$(3,7,5,11)$	3.3912	II	0.0899
$(4,7,5,11)$	3.5296	I	0.0731
$(5,9,7,11)$	3.9195	I	0.0510
$(5,8,9,11)$	3.9838	II	0.0611
$(9,10,11,13)$	4.5506	II	0.0336
$(11,13,14,15)$	4.9580	II	0.0276

$$\zeta_{\mathcal{C}^{(2)}}(P,Q,R,S)=\frac{1}{2}\min_{\substack{\delta_p\in(-P,P),\delta_q\in(-Q,Q),\\ \delta_r\in(-R,R),\delta_s\in(-S,S)\\ (\delta_p,\delta_q,\delta_r,\delta_s)\neq(0,0,0,0)}}\left|2\mathcal{I}m[(\Theta_1-\bar{\Theta}_1 w)(\bar{\Theta}_2-\Theta_2 x)]\right|^{1/3}. \quad (18)$$

TABLE III
DIVERSITY PRODUCTS OF SOME GROUP-BASED CODES AND THE NONGROUP CODE

Group	Rate	$\frac{1}{2}\min\lvert\det(U_i-U_j)\rvert^{1/3}$
cyclic group with $u=(1,17,26)$	1.99	0.3301
cyclic group with $u=(1,11,27)$	2	0.2765
$G_{21,4}$	1.99	0.3851
$G_{171,64}$	3	0.1353
$G_{1365,16}$	4	0.0361
$G_{10815,46}$	5	0.0131
products of groups with $L_A=65, u=(1,30,114)$	4.01	0.0933

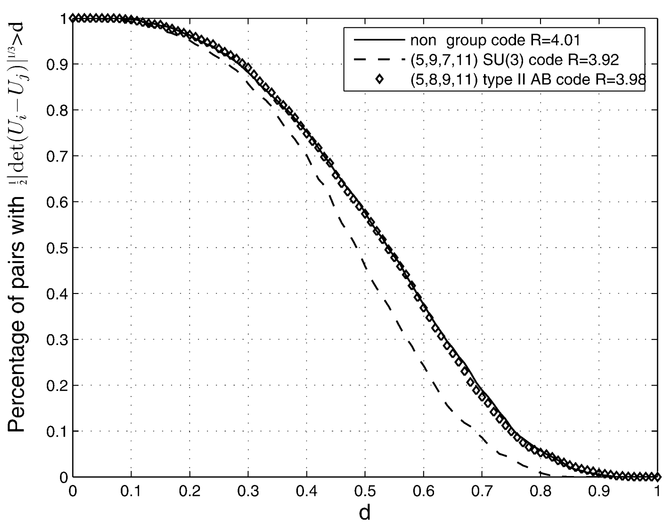


Fig. 1. Comparison of distributions of AB, $SU(3)$, and the nongroup codes at rate approximately 4.

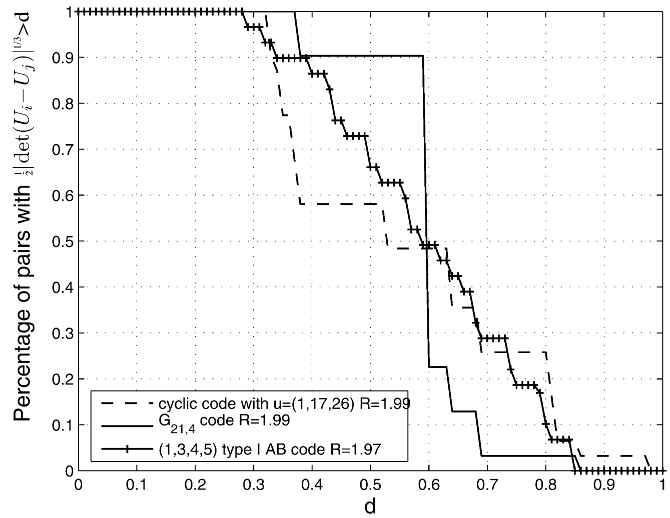


Fig. 2. Comparison of distributions of AB code and group codes at rate approximately 2.

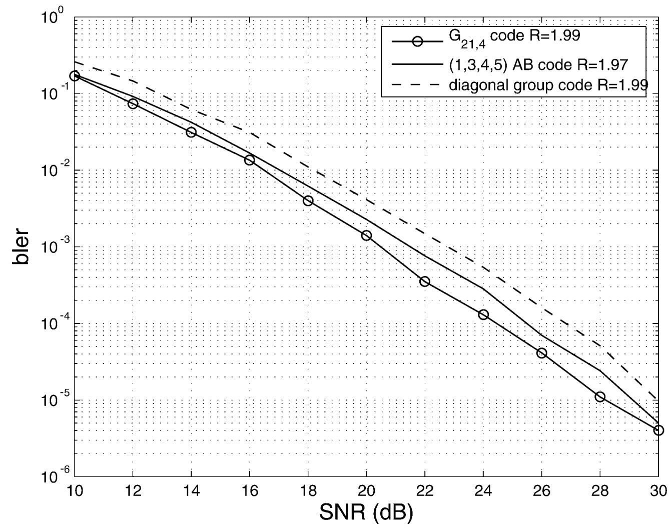


Fig. 3. Comparison of the rate 1.9690, (1,3,4,5) type I AB code with the rate 1.99 $G_{21,4}$ code and the best rate 1.99 cyclic group code. The number of receive antennas is one.

one nongroup code designed in [4], as given in Table III. We can see from the tables that diversity products of the $SU(3)$ and AB codes are about the same as those of group-based codes at low rates, but when the rates are high, diversity products of $SU(3)$ and AB codes are much greater than those of group-based codes at about the same rates. The diversity product of the $SU(3)$ code at rate 3.9195, which is 0.0510, is smaller than that of the nongroup code at rate 4.01, which is 0.0933. However, simulated performance in Section VI shows that the code performs only slightly worse than the nongroup code. In addition, the diversity product of the (5,8,9,11) AB code at rate 3.9838, which is 0.0611, is again smaller than that of the nongroup code, but simulations in Section VI show that the code performs as well as the nongroup code.

To explain this, we plot distributions of $(1/2)|\det(U_i - U_j)|1/3$ over all pairs of codewords for the three codes in Fig. 1. The plot shows the percentage of pairs whose $(1/2)|\det(U_i - U_j)|1/3$ is larger than d. As can be seen from the plot, distributions of matrices in the AB code and the nongroup code are almost identical, whereas the $SU(3)$ code has a slightly worse distribution. We also show distributions of the three codes at a rate of approximately 2: the (1,3,4,5) type I AB code, the diagonal group-based code with $u=[1,17,26]$, and the $G_{21,4}$ code. As can be seen from Fig. 2, the $G_{21,4}$ code, which has the highest diversity product, has the best distribution as well. Although the diagonal group code has a higher diversity product than the AB code, it has more pairs with low $(1/2)|\det(U_i - U_j)|1/3$. This is consistent with the simulated performance of the three codes in Fig. 3, where the $G_{21,4}$ code has the best performance, and the diagonal code has the worst. We should note that the distribution of $(1/2)|\det(U_i - U_j)|1/3$ is simply used for better understanding of our codes. We cannot envision how to use it for code design.

Theorem 6 (Necessary Condition for Fully Diverse): A necessary condition for type I AB code to be fully diverse is that every pair of the four integers $\{P,Q,R,S\}$ is relatively prime. A necessary condition for type II AB code to be fully diverse is $\gcd(P,Q)=\gcd(R,S)=1$, and at most one of the four integers $\{P,Q,R,S\}$ is even.

Proof: See Appendix E. □

Note that for type II AB codes, that every pair of the four integers $\{P,Q,R,S\}$ is relatively prime is not a necessary condition. By simulations, $\zeta_{\mathcal{C}^{(2)}}(3,5,3,5) = 0.1706 > 0$ and $\zeta_{\mathcal{C}^{(2)}}(7,9,7,9) = 0.0219 > 0$, which indicates that $\gcd(P,R)=1$, $(P,S)=1$, $\gcd(Q,R)=1$, or $\gcd(Q,S)=1$ is not necessary for the code to be fully diverse. We are not able to give sufficient conditions for full diversity of AB codes. Based on the diversity product given in (18) and simulations, our conjecture is that the necessary conditions are also sufficient.

V. Fast Decoding Algorithm for AB Codes

From (9) and (16), we can see that any matrix in code $\mathcal{C}^{(2)}_{(P,Q,R,S)}$ is a product of two unitary matrices $A^{(2)}_{(p,q)}$ and $B^{(2)}_{(r,s)}$. It is easy to see from (14) that the two matrices have an orthogonal design structure. This handy property can be used to get linear-algebraic decoding, which means that the receiver can be made to form a system of linear equations in the unknowns.

The ML decoding for differential USTM given in (4) is equivalent to

$$\arg\min_{p,q,r,s}\left\|X_\tau - A^{(2)}_{(p,q)}B^{(2)}_{(r,s)}X_{\tau-1}\right\|_F^2 = \arg\min_{p,q,r,s}\left\|A^{(2)*}_{(p,q)}X_\tau - B^{(2)}_{(r,s)}X_{\tau-1}\right\|_F^2.$$

Therefore, the decoding formula for code $\mathcal{C}^{(2)}_{(P,Q,R,S)}$ can be written as the equation shown at the bottom of the page, where $x_{t,ij}$ indicates the (i,j)th entry of the $M\times N$ matrix X_t for $t=\tau,\tau-1$. The equality is obtained since $A^{(2)}_{(p,q)}$ and $B^{(2)}_{(r,s)}$ have orthogonal structure. It is easy to see that the formula inside the norm is linear in the PSK unknown signals. Therefore, we can use sphere decoding for complex channels proposed in [15] with slight modification. The only difference here is that the unknowns $e^{-j\theta'_{p,q}}$ and $e^{-j\xi'_{r,s}}$ are not independent unknown PSK signals but are determined by $e^{2\pi j(p/P)}$, $e^{-2\pi j(q/Q)}$ and $e^{2\pi j(r/R)}$, $e^{2\pi j(s/S)}$. Therefore, in the sphere decoder, instead of searching over possible intervals for $e^{-j\theta'_{p,q}}$ and $e^{-j\xi'_{r,s}}$, we calculate their values by values of p, q and r, s, respectively, based on (15), depending on the choices of $\theta'_{p,q}$ and $\xi'_{r,s}$. Since sphere decoding has an average complexity that is cubic in both the code rate and dimension of the system and, at the same time, achieves the ML result, we find a fast decoding algorithm for AB codes.

In digital communication, the choice of the searching radius is very crucial to the speed of the algorithm. If the initial radius is chosen to be very large, then we are actually searching most of the points by which not too much improvement on computational complexity can be gained over exhaustive search. On the other hand, if the radius is chosen to be too small, then there may be no point in the sphere that we are searching. It is better to start with a small value and then increase it gradually. In [16], the authors proposed to chose the packing radius or the estimated packing radius to be the initial searching radius. In this paper, we use another initialization based on the noise level, as in [8] and [17]. The noise of the system is given in (3). Since W_τ, $W_{\tau-1}$, and the data matrix U_{z_τ} are independent, it is easy to prove that the noise matrix has mean zero and variance $2NI_3$. Each component of the $3\times N$ noise matrix has mean zero and variance 2. Therefore, the random variable $v = \|W'_\tau\|_F^2$ has a χ^2 distribution with mean $3N$. We initialize the searching radius $\sqrt{C}$ such that the probability that the correct signal is in the sphere is 0.9, that is, $P(\|v\|_F < \sqrt{C}) = 0.9$. If no point is found in the sphere, then we raise the searching radius to have the probability increased to 0.99, and so on. Using this algorithm, the probability that we can find a point during the first search is high. For more details of sphere decoding for real and complex systems, see [15] and [16].

Although $SU(3)$ codes also have the structure of products of two unitary matrices, since the two unitary matrices do not have orthogonal design structure, we cannot find a way to simplify the decoding. Therefore, for $SU(3)$ codes, exhaustive search is used to obtain the ML results.

VI. Simulation Results

In this section, we give examples of both $SU(3)$ codes and the two types of AB codes, as well as the simulated performance of the codes for different rates. The number of transmit antennas is three. The fading coefficient from each transmit antenna to each receive antenna is modeled independently as a complex Gaussian variable with mean zero and variance one and keeps constant for $2M=6$ channel uses. At each channel use, zero-mean, unit-variance complex Gaussian noise is added to each receive antenna. The block error rate (bler), which corresponds to errors in decoding the 3×3 transmit matrices, is demonstrated as the error event of interest. We also compare the performance of the proposed codes with that of group-based codes and the nongroup code in [4].

$$\arg\max_{p,q,r,s}\left\|\begin{bmatrix} x_{\tau,11} & 0 & 0 & 0 & -\frac{x_{\tau-1,11}}{\sqrt{2}} & -\frac{x_{\tau-1,21}}{\sqrt{2}} \\ 0 & \frac{\bar{x}_{\tau,21}}{\sqrt{2}} & -\frac{\bar{x}_{\tau,31}}{\sqrt{2}} & 0 & -\frac{\bar{x}_{\tau-1,21}}{\sqrt{2}} & \frac{\bar{x}_{\tau-1,11}}{\sqrt{2}} \\ 0 & \frac{x_{\tau,31}}{\sqrt{2}} & \frac{x_{\tau,21}}{\sqrt{2}} & -x_{\tau-1,31} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{\tau,1N} & 0 & 0 & 0 & -\frac{x_{\tau-1,1N}}{\sqrt{2}} & -\frac{x_{\tau-1,2N}}{\sqrt{2}} \\ 0 & \frac{\bar{x}_{\tau,2N}}{\sqrt{2}} & -\frac{\bar{x}_{\tau,3N}}{\sqrt{2}} & 0 & -\frac{\bar{x}_{\tau-1,2N}}{\sqrt{2}} & \frac{\bar{x}_{\tau-1,1N}}{\sqrt{2}} \\ 0 & \frac{x_{\tau,3N}}{\sqrt{2}} & \frac{x_{\tau,2N}}{\sqrt{2}} & -x_{\tau-1,3N} & 0 & 0 \end{bmatrix}\begin{bmatrix} e^{-j\theta'_{p,q}} \\ e^{2\pi j(p/P)} \\ e^{-2\pi j(q/Q)} \\ e^{-j\xi'_{r,s}} \\ e^{2\pi j(r/R)} \\ e^{2\pi j(s/S)} \end{bmatrix}\right\|_F^2$$

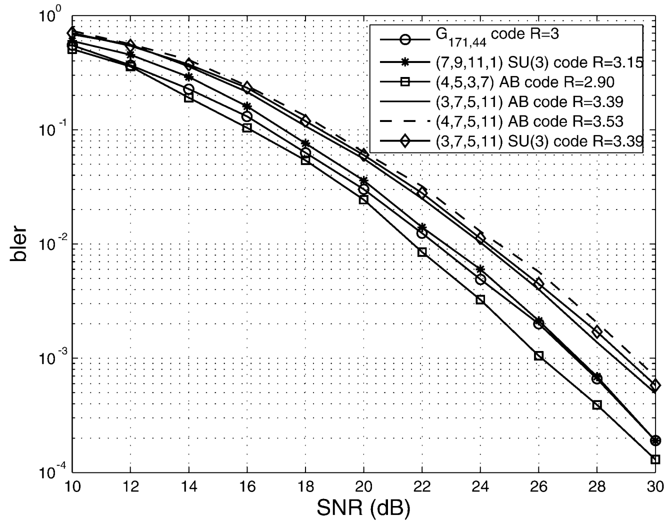


Fig. 4. Comparison of 1) the rate 2.9045, (4,5,3,7) type I AB code, 2) the rate 3.15, (7,9,11,1) $SU(3)$ code, 3) the rate 3.3912, (3,7,5,11) type II AB code, 4) the rate 3.5296, (4,7,5,11) type I AB code, and 5) the rate 3.3912, (3,7,5,11), $SU(3)$ code with 6) the rate 3, $G_{171,64}$ code. The number of receive antennas is 1.

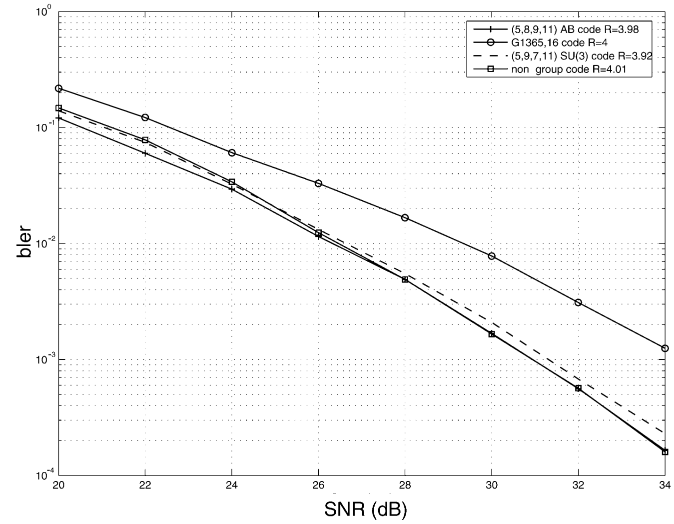


Fig. 5. Comparison of 1) the rate 3.9838, (5,8,9,11) type II AB code and 2) the rate 3.9195,(5,9,7,11), $SU(3)$ code with 3) the rate 4 $G_{1365,16}$ code. The number of receive antennas is 1.

A. AB Code versus Group-Based Codes at $R \approx 2$

The first example is the $P = 1$, $Q = 3$, $R = 4$, and $S = 5$ AB code with $\theta_{p,q} = 2\pi(-p/P + q/Q)$ and $\xi_{r,s} = 2\pi(-r/R - s/S)$. In brief, we call it the (1,3,4,5) type I AB code. From (10), the rate of the code is 1.9690. From Table II, the diversity product of the code is 0.2977. We compare its bler with the $G_{21,4}$ group code at rate $R = 1.99$ with diversity product 0.3851 as well as the best cyclic group code with $u = (1, 17, 26)$ at rate 1.99, whose diversity product is 0.3301. The number of receive antennas is one. The performance curves are shown in Fig. 3. From the plot, we can see that performances of the three codes are close to each other. The AB code is a little (about 1 dB) worse than the $G_{21,4}$ code and better (about 1 dB) than the cyclic group code. Notice that decoding of both group-based codes needs exhaustive search, but the AB code has a fast decoding method. Therefore, at rate of approximately 2, the AB code is as good as the group-based codes with far superior decoding complexity.

B. $SU(3)$ and AB Codes versus Group-Based Codes at $R \approx 3$

In this subsection, we compare two sets of codes. The first set includes the (4,5,3,7) type I AB code with rate $R = 2.9045$, the $G_{171,64}$ group-based code at rate 3, and the $SU(3)$ code with $(P, Q, R, S) = (7, 9, 11, 1)$ and rate 3.1456. The number of receive antennas is one. The simulated blers are shown in Fig. 4. From the plot, we can see that the AB code is about 1 dB better than the $G_{171,64}$ code. The $SU(3)$ code has about the same performance as the group-based code with a 0.1456 higher rate.

The second set of codes are the (3,7,5,11) type II AB code at rate $R = 3.3912$, the (4,7,5,11) type I AB code with rate $R = 3.5296$, and the (3,7,5,11), $SU(3)$ code with rate $R = 3.3912$. The number of receive antennas is one. The simulated blers are shown in Fig. 4. The three codes have very close performance. Compared with the performance of the $G_{171,64}$ code, which is shown by the line with circles, the three codes, the two AB codes, and the $SU(3)$ code with rates 0.3912, 0.5296, and 0.3912 higher are about 1.5 dB worse. Note that the AB code can be decoded much faster than the $G_{171,64}$ code and the $SU(3)$ code.

C. $SU(3)$ and AB Codes versus Group-Based Codes and the Nongroup Code at $R \approx 4$

Comparison of the (5,8,9,11) type II AB code at rate 3.9838 and the (5,9,7,11) $SU(3)$ code at rate 3.9195 with the rate 4 group-based $G_{1365,16}$ code is given in Fig. 5. The number of receive antennas is one. We can see that at about the same rate, the AB code and the $SU(3)$ code perform a lot better than the $G_{1365,16}$ code. For example, at a bler of 10^{-2}, both codes have an advantage of about 3 dB, and the advantage increases as SNR increases. We also give the performance of the nongroup code, which is indicated by the line with squares. From the plot, we can see that the AB and $SU(3)$ codes are as good as and comparable to the nongroup code given in [4].

In Fig. 6, the (9,10,11,13) type II AB code at rate 4.5506 and the (7,11,9,13) $SU(3)$ code at rate 4.3791 are compared with the rate 4 group-based $G_{1365,16}$ code. As can be seen in Fig. 6, at high SNR, with the higher rate 0.3791, the $SU(3)$ code performs more than 1 dB better than the $G_{1365,16}$ code, and the AB code has a performance that is slightly better than the $G_{1365,16}$ code, even with a rate that is 0.5506 higher.

These two plots show that both the AB and $SU(3)$ codes give a much better performance than the group-based code. They even have the same good performance as the elaborately designed nongroup code. Another advantage is that AB codes have a fast decoding algorithm, whereas the decoding of both group-based and the nongroup codes needs exhaustive search.

D. AB Code versus Group-Based Code at Higher Rates

In this subsection, we compare the (11,13,14,15) type II AB code with the $G_{10815,46}$ group-based code. The rate of the AB code is 4.9580, and the rate of the group-based code is 5. The

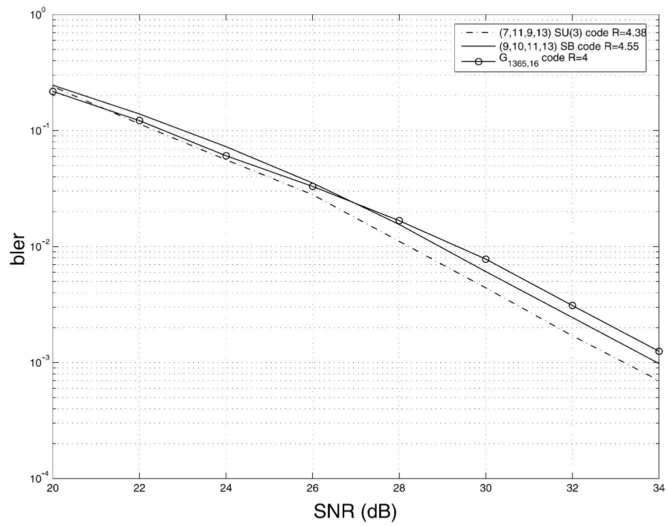


Fig. 6. Comparison of 1) the rate 4.55.6, (9,10,11,13) type II AB code and 2) the rate 4.3791, (7,11,9,13), $SU(3)$ code with 3) the rate 4 $G_{1365,16}$ code and 4) the rate 4 nongroup code. The number of receive antennas is 1.

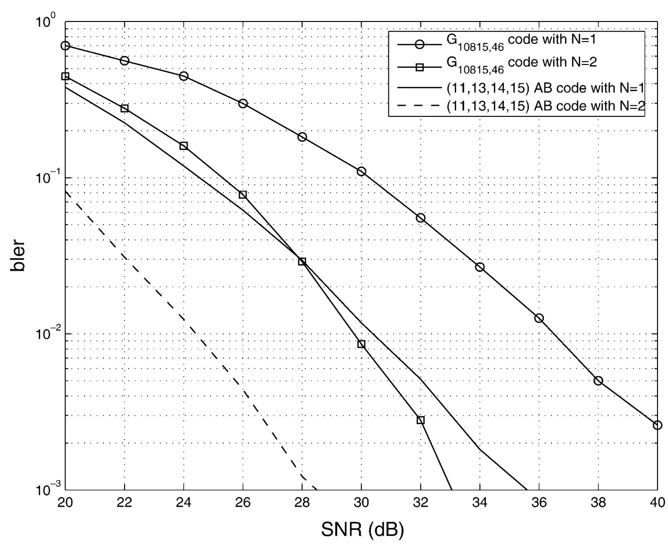


Fig. 7. Comparison of the rate 4.9580, (11,13,14,15) type II AB code with the rate 5 $G_{10815,46}$ code. The number of receive antennas is 1 and 2.

simulated blers are shown in Fig. 7. The line with circles indicates the bler of the $G_{10815,46}$ code, and the solid line shows the bler of the AB code with one receive antenna. The plot shows that the AB code gives a much better performance. For example, at the bler of 10^{-2}, the AB code is 6 dB better, and the performance gap is even higher for lower blers or higher SNRs. In this plot, we also give examples with two receive antennas. The line with squares indicates the bler of the $G_{10815,46}$ code, and the dashed line indicates the bler of the AB code. Again, we can see that the AB code is much better than the group-based code. As mentioned before, the AB codes have a fast decoding algorithm, whereas decoding the group-based codes needs exhaustive search. Therefore, at high rates, AB codes have great advantages over group-based codes in both performance and decoding complexity.

VII. Conclusion

In this paper, we worked with the special unitary Lie group $SU(3)$, which has dimension 8 and rank 2. The group is not fixed-point-free, but we describe a method to design fully diverse codes that are subsets of the group. Furthermore, motivated by the structure of the proposed $SU(3)$ codes, we propose a simpler code called the AB code. Both codes are suitable for systems with three transmit antennas. Necessary conditions for the full diversity of both codes are given, and our conjecture is that they are also sufficient conditions. The codes have simple formulas from which their diversity products can be calculated in a fast way. A fast maximum-likelihood decoding algorithm for AB codes based on complex sphere decoding is given, whose complexity is polynomial in the rate and dimension. Simulation results show that $SU(3)$ and AB codes perform as well as finite group-based codes at low rates, but they do not need the exhaustive search (of exponentially growing size) required of group-based codes and, therefore, are far superior in terms of decoding complexity. $SU(3)$ and AB codes have great advantages over finite group-based codes at high rates and perform as well as the carefully designed nongroup code in addition to the superiority (by far) in decoding complexity of the AB codes.

Appendix A
Proof of Theorem 1

Proof: It is easy to prove that any matrix U that satisfies (5) is in $SU(3)$ by checking that $UU^* = I_3$ and $\det U = 1$. Now, we need to prove that any matrix $U \in SU(3)$ can be written as (5). Partition U into $\begin{bmatrix} a & U_{12} \\ U_{21} & U_{22} \end{bmatrix}$, where a is a complex number, U_{12} is 1×2, U_{21} is 2×1, and U_{22} is 2×2. Since $UU^* = I_3$

$$\begin{bmatrix} a & U_{12} \\ U_{21} & U_{22} \end{bmatrix} \begin{bmatrix} \bar{a} & U_{21}^* \\ U_{12}^* & U_{22}^* \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{0}_{12} \\ \mathbf{0}_{21} & I_2 \end{bmatrix}.$$

Comparing the (1,1) entries, we have $U_{12}U_{12}^* = 1 - |a|^2$. Therefore, $|a|^2 < 1$. Comparing the (1,2) entries, we have

$$aU_{21}^* + U_{12}U_{22}^* = \mathbf{0}_{12} \Rightarrow U_{21}^* = -a^{-1}U_{12}U_{22}^*.$$

Comparing the (2,2) entries

$$\begin{aligned} U_{21}U_{21}^* + U_{22}U_{22}^* &= I_2 \Rightarrow -a^{-1}U_{21}U_{12}U_{22}^* + U_{22}U_{22}^* \\ &= I_2 \Rightarrow a^{-1}U_{21}U_{12} = U_{22} - U_{22}^{-*}. \end{aligned}$$

For any matrix A, A^{-*} indicates the inverse of A^*.

Now let us look at the unit determinant constraint.

$$\begin{aligned} 1 = \det U &= a \cdot \det(U_{22} - U_{21}a^{-1}U_{12}) \\ &= a \cdot \det U_{22}^{-*} = a(\overline{\det U_{22}})^{-1}. \end{aligned}$$

Therefore, $\det U_{22} = \bar{a}$. From $U_{21}U_{21}^* + U_{22}U_{22}^* = I_2$, we know that $I_2 - U_{22}U_{22}^*$ has rank 1. Therefore, 1 is an eigenvalue of $U_{22}U_{22}^*$. The other eigenvalue must be $|a|^2$ since $\det U_{22}U_{22}^* = |a|^2$. Thus, the Hermitian and positive matrix $U_{22}U_{22}^*$ can be decomposed as $U_{22}U_{22}^* = \Phi \begin{bmatrix} 1 & 0 \\ 0 & |a|^2 \end{bmatrix} \Phi^*$ for some unitary matrix Φ with determinant 1. Therefore, there exists a unitary matrix Ψ with determinant 1 such that $U_{22} = \Phi \begin{bmatrix} 1 & 0 \\ 0 & \bar{a} \end{bmatrix} \Psi$.

Again, from $U_{21}U_{21}^* + U_{22}U_{22}^* = I_2$

$$\begin{aligned} U_{21}U_{21}^* &= I_2 - U_{22}U_{22}^* = \Phi \begin{bmatrix} 0 & 0 \\ 0 & 1-|a|^2 \end{bmatrix} \Phi^* \\ &= \Phi \begin{bmatrix} 0 \\ \sqrt{1-|a|^2}e^{j\chi} \end{bmatrix} [\,0 \quad \sqrt{1-|a|^2}e^{-j\chi}\,]\, \Phi^*. \end{aligned}$$

A general solution for U_{21} is

$$U_{21} = \Phi \left[0, \sqrt{1-|a|^2}e^{j\chi}\right]^T$$

where A^T indicates the transpose of A. χ is an arbitrary angle. By a similar argument, a general solution for U_{12} is

$$U_{12} = [\,0 \quad \sqrt{1-|a|^2}e^{j\eta}\,]\, \Psi$$

where η is an arbitrary angle. In addition

$$\begin{aligned} aU_{21}^* + U_{12}U_{22}^* &= 0 \\ &\Rightarrow a\,[\,0 \quad \sqrt{1-|a|^2}e^{-j\chi}\,]\, \Phi^* \\ &\quad + [\,0 \quad \sqrt{1-|a|^2}e^{j\eta}\,]\, \Psi\Psi^* \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} \Phi^* \\ &= 0 \\ &\Rightarrow e^{j\eta} = -e^{-j\chi}. \end{aligned}$$

Therefore, we have proved that matrices in $SU(3)$ have the following structure.

$$\begin{aligned} &\begin{bmatrix} a & [\,0 \quad -\sqrt{1-|a|^2}e^{-j\chi}\,]\, \Psi \\ \Phi \begin{bmatrix} 0 \\ \sqrt{1-|a|^2}e^{j\chi} \end{bmatrix} & \Phi \begin{bmatrix} 1 & 0 \\ 0 & \bar{a} \end{bmatrix} \Psi \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & \Phi \end{bmatrix} \\ &\times \begin{bmatrix} \bar{a} & 0 & -\sqrt{1-|a|^2}e^{-j\chi} \\ 0 & 1 & 0 \\ \sqrt{1-|\alpha|^2}e^{j\chi} & 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \Psi \end{bmatrix}. \end{aligned}$$

Since

$$\begin{aligned} &\begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-j\beta} & 0 \\ 0 & 0 & e^{j\beta} \end{bmatrix} \begin{bmatrix} a & 0 & -\sqrt{1-|a|^2}e^{-j\chi} \\ 0 & 1 & 0 \\ \sqrt{1-|a|^2}e^{j\chi} & 0 & \bar{a} \end{bmatrix} \\ &\times \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{j\beta} & 0 \\ 0 & 0 & e^{-j\beta} \end{bmatrix} \\ &= \begin{bmatrix} a & 0 & -\sqrt{1-|a|^2}e^{-j(\chi+\beta)} \\ 0 & 1 & 0 \\ \sqrt{1-|a|^2}e^{j(\chi+\beta)} & 0 & \bar{a} \end{bmatrix} \end{aligned}$$

for any real angle β, the angle χ is a redundant degree of freedom. Therefore, we can set $\chi = 0$. Equation (5) is thus obtained. □

APPENDIX B
PROOF OF THEOREM 2

Proof: Define $\theta_i = 2\pi\,(p_i/P - q_i/Q)$ and $\xi_i = 2\pi\,(r_i/R + s_i/S)$ for $i = 1, 2$. Furthermore, define $\gamma_1 = 2\pi\,((p_1-p_2)/2P + (q_1-q_2)/2Q)$ and $\gamma_2 = 2\pi\,((r_1-r_2)/2R - (s_1-s_2)/2S)$. For any $U_1(p_1,q_1,r_1,s_1)$ and $U_2(p_2,q_2,r_2,s_2)$ in $\mathcal{C}^{(1)}$, $U_1 = A^{(1)}_{(p_1,q_1)}B^{(1)}_{(r_1,s_1)}$ and $U_2 = A^{(1)}_{(p_2,q_2)}B^{(1)}_{(r_2,s_2)}$, where $A^{(1)}$ and $B^{(1)}$ are as defined in (8). We then have the first equation at the top of the next page. Therefore, we have the second equation on the next page.

Define the equation at the top of the page that is two pages after this page. The equation following the definition can thus be obtained. □

APPENDIX C
PROOF OF THEOREM 3

Proof: First, we prove that $\gcd(P,Q) = 1$ is a necessary condition for the set $\left\{A^{(1)}_{(p,q)}\right\}$ to be fully diverse and thus a necessary condition for full diversity of the code. Let

$$\begin{aligned} A^{(1)}_{(p_1,q_1)} &= \begin{bmatrix} e^{j\theta_1} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p_1/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_1/Q)}e^{-j\theta_1} \\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q_1/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_1/P)}e^{-j\theta_1} \end{bmatrix} \\ A^{(1)}_{(p_2,q_2)} &= \begin{bmatrix} e^{j\theta_2} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p_2/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_2/Q)}e^{-j\theta_2} \\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q_2/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_2/P)}e^{-j\theta_2} \end{bmatrix} \end{aligned}$$

where $\theta_1 = 2\pi(p_1/P - q_1/Q)$, and $\theta_2 = 2\pi(-p_2/P - q_2/Q)$. We then have

$$\det\left(A^{(1)}_{(p_1,q_1)} - A^{(1)}_{(p_2,q_2)}\right) = \left(e^{j\theta_1} - e^{j\theta_2}\right) X$$

for some X. If $\gcd(P,Q) = G > 1$, let $0 \le p_1 = p_2 + P/G < P$, and $0 \le q_1 = q_2 + Q/G < Q$.

$$e^{j\theta_1} - e^{j\theta_2} = e^{2\pi j((p_2/P)-(q_2/Q))} - e^{2\pi j(p_2/P - q_2/Q)} = 0.$$

Therefore, $\gcd(P,Q) = 1$ is a necessary condition for the set $\left\{A^{(1)}_{(p,q)}\right\}$ to be fully diverse. By a similar argument, $\gcd(R,S) = 1$ is also a necessary condition.

Now, assume $\gcd(P,R) = G > 1$. Let $q_1 = q_2$, $s_1 = s_2$, $0 \le p_1 = p_2 + P/G$, and $0 \le r_1 = r_2 + R/G$. From (11), $x = e^{j(\pi/G)}\cos(\pi/G)$, $w = e^{-j(\pi/G)}\cos(\pi/G)$, and $\Theta = e^{j(4\pi/G)}$. Therefore, for the two matrices $U_1(p_1,q_1,r_1,s_1)$ and $U_2(p_2,q_2,r_2,s_2)$ in $\mathcal{C}^{(1)}$

$$\begin{aligned} &\det\left(U_1(p_1,q_1,r_1,s_1) - U_2(p_2,q_2,r_2,s_2)\right) \\ &\quad = 2j(\mathcal{I}m(wx) - \mathcal{I}m\bar{\Theta}x - \mathcal{I}m\Theta w) \\ &\quad = 2j\bigg(-\cos 2\pi\frac{1}{2G}\sin 2\pi\frac{5}{2G} \\ &\qquad\qquad - \cos 2\pi\frac{1}{2G}\sin 2\pi\left(-\frac{5}{2G}\right)\bigg) \\ &\quad = 0. \end{aligned}$$

$\mathcal{C}^{(1)}$ is not fully diverse, which means that $\gcd(P,R) = 1$ is a necessary condition. From the symmetry of P and Q, R and S, $\gcd(P,S) = \gcd(Q,R) = \gcd(Q,S) = 1$ are also necessary. Therefore, every two of the four integers $\{P,Q,R,S\}$ that are relatively prime are necessary for code $\mathcal{C}^{(1)}$ to be fully diverse.

$$
\begin{aligned}
\left(A^{(1)}_{(p_2,q_2)}\right)^{-1} A^{(1)}_{(p_1,q_1)} &= \begin{bmatrix} e^{-j\theta_2} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{-2\pi j(p_2/P)} & -\frac{1}{\sqrt{2}}e^{2\pi j(q_2/Q)} \\ 0 & \frac{1}{\sqrt{2}}e^{-2\pi j(q_2/Q)}e^{j\theta_2} & \frac{1}{\sqrt{2}}e^{2\pi j(p_2/P)}e^{j\theta_2} \end{bmatrix} \begin{bmatrix} e^{j\theta_1} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{2\pi j(p_1/P)} & \frac{1}{\sqrt{2}}e^{2\pi j(q_1/Q)}e^{-j\theta_1} \\ 0 & -\frac{1}{\sqrt{2}}e^{-2\pi j(q_1/Q)} & \frac{1}{\sqrt{2}}e^{-2\pi j(p_1/P)}e^{-j\theta_1} \end{bmatrix} \\
&= \begin{bmatrix} e^{j(\theta_1-\theta_2)} & 0 & 0 \\ 0 & \frac{1}{2}\left(e^{2\pi j(p_1-p_2)/P}+e^{-2\pi j(q_1-q_2)/Q}\right) & \frac{1}{2}\left(e^{2\pi j(-p_2/P+q_1/Q)}-e^{2\pi j(-p_1/P+q_2/Q)}\right)e^{-j\theta_1} \\ 0 & \frac{1}{2}\left(e^{2\pi j(p_1/P-q_2/Q)}-e^{2\pi j(p_2/P-q_1/Q)}\right)e^{j\theta_2} & \frac{1}{2}\left(e^{-2\pi j(p_1-p_2)/P}+e^{2\pi j(q_1-q_2)/Q}\right)e^{-j(\theta_1-\theta_2)} \end{bmatrix} \\
&= \begin{bmatrix} e^{j(\theta_1-\theta_2)} & 0 & 0 \\ 0 & e^{2\pi j((p_1-p_2)/2P-(q_1-q_2)/2Q)}\cos\gamma_1 & e^{-j\theta_1}je^{2\pi j(-(p_1+p_2)/2P+(q_1+q_2)/2Q)}\sin\gamma_1 \\ 0 & e^{j\theta_2}je^{2\pi j((p_1+p_2)/2P-(q_1+q_2)/2Q)}\sin\gamma_1 & e^{-j(\theta_1-\theta_2)}e^{2\pi j(-(p_1-p_2)/2P+(q_1-q_2)/2Q)}\cos\gamma_1 \end{bmatrix} \\
&= \begin{bmatrix} e^{-j\theta_2} & 0 & 0 \\ 0 & e^{2\pi j(-p_2/2P+q_2/2Q)} & 0 \\ 0 & 0 & e^{j\theta_2}e^{2\pi j(p_2/2P-q_2/2Q)} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma_1 & j\sin\gamma_1 \\ 0 & j\sin\gamma_1 & \cos\gamma_1 \end{bmatrix} \\
&\quad\times \begin{bmatrix} e^{j\theta_1} & 0 & 0 \\ 0 & e^{2\pi j(p_1/2P-q_1/2Q)} & 0 \\ 0 & 0 & e^{-j\theta_1}e^{2\pi j(-p_1/2P+q_1/2Q)} \end{bmatrix}
\end{aligned}
$$

and

$$
\begin{aligned}
B^{(1)}_{(r_2,s_2)}\left(B^{(1)}_{(r_1,s_1)}\right)^{-1} &= \begin{bmatrix} \frac{1}{\sqrt{2}}e^{2\pi j(r_2/R)}e^{j\xi_2} & \frac{1}{\sqrt{2}}e^{2\pi j(s_2/S)}e^{j\xi_2} & 0 \\ -\frac{1}{\sqrt{2}}e^{-2\pi j(s_2/S)} & \frac{1}{\sqrt{2}}e^{-2\pi j(r_2/R)} & 0 \\ 0 & 0 & e^{-j\xi_2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}}e^{-2\pi j(r_1/R)}e^{-j\xi_1} & -\frac{1}{\sqrt{2}}e^{2\pi j(s_1/S)} & 0 \\ \frac{1}{\sqrt{2}}e^{-2\pi j(s_1/S)}e^{-j\xi_1} & \frac{1}{\sqrt{2}}e^{2\pi j(r_1/R)} & 0 \\ 0 & 0 & e^{j\xi_1} \end{bmatrix} \\
&= \begin{bmatrix} \frac{1}{2}\left(e^{-2\pi j(r_1-r_2)/R}+e^{-2\pi j(s_1-s_2)/S}\right)e^{-j(\xi_1-\xi_2)} & \frac{1}{2}\left(e^{2\pi j(r_1/R+s_2/S)}-e^{2\pi j(r_2/R+s_1/S)}\right)e^{j\xi_2} & 0 \\ \frac{1}{2}\left(e^{2\pi j(-r_2/R-s_1/S)}-e^{2\pi j(-r_1/R-s_2/S)}\right)e^{-j\xi_1} & \frac{1}{2}\left(e^{2\pi j(r_1-r_2)/R}+e^{2\pi j(s_1-s_2)/S}\right) & 0 \\ 0 & 0 & e^{j(\xi_1-\xi_2)} \end{bmatrix} \\
&= \begin{bmatrix} e^{-j(\xi_1-\xi_2)}e^{2\pi j(-(r_1-r_2)/2R-(s_1-s_2)/2S)}\cos\gamma_2 & je^{j\xi_2}e^{2\pi j((r_1+r_2)/2R+(s_1+s_2)/2S)}\sin\gamma_2 & 0 \\ je^{-j\xi_1}e^{2\pi j(-(r_1+r_2)/2R-(s_1+s_2)/2S)}\sin\gamma_2 & e^{2\pi j((r_1-r_2)/2R+(s_1-s_2)/2S)}\cos\gamma_2 & 0 \\ 0 & 0 & e^{j(\xi_1-\xi_2)} \end{bmatrix} \\
&= \begin{bmatrix} e^{j\xi_2}e^{2\pi j(r_2/2R+s_2/2S)} & 0 & 0 \\ 0 & e^{2\pi j(-r_2/2R-s_2/2S)} & 0 \\ 0 & 0 & e^{-j\xi_2} \end{bmatrix} \begin{bmatrix} \cos\gamma_2 & j\sin\gamma_2 & 0 \\ j\sin\gamma_2 & \cos\gamma_2 & \\ 0 & 0 & 1 \end{bmatrix} \\
&\quad\times \begin{bmatrix} e^{-j\xi_1}e^{2\pi j(-r_1/2R-s_1/2S)} & 0 & 0 \\ 0 & e^{2\pi j(r_1/2R+s_1/2S)} & 0 \\ 0 & 0 & e^{j\xi_1} \end{bmatrix}.
\end{aligned}
$$

$$
\begin{aligned}
\det(U_1(p_1,q_1,r_1,s_1)-U_2(p_2,q_2,r_2,s_2) &= \det A^{(1)}_{(p_2,q_2)}\det B^{(1)}_{(r_1,s_1)}\det\left(\left(A^{(1)}_{(p_2,q_2)}\right)^{-1}A^{(1)}_{(p_1,q_1)}-B^{(1)}_{(r_2,s_2)}\left(B^{(1)}_{(r_1,s_1)}\right)^{-1}\right) \\
&= \det\left(\begin{bmatrix} e^{-j\theta_2} & 0 & 0 \\ 0 & e^{2\pi j(-p_2/2P+q_2/2Q)} & 0 \\ 0 & 0 & e^{j\theta_2}e^{2\pi j(p_2/2P-q_2/2Q)} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma_1 & j\sin\gamma_1 \\ 0 & j\sin\gamma_1 & \cos\gamma_2 \end{bmatrix}\right. \\
&\qquad\times \begin{bmatrix} e^{j\theta_1} & 0 & 0 \\ 0 & e^{2\pi j(p_1/2P-q_1/2Q)} & 0 \\ 0 & 0 & e^{-j\theta_1}e^{2\pi j(-p_1/2P+q_1/2Q)} \end{bmatrix} \\
&\qquad- \begin{bmatrix} e^{j\xi_2}e^{2\pi j(r_2/2R+s_2/2S)} & 0 & 0 \\ 0 & e^{2\pi j(-r_2/2R-s_2/2S)} & 0 \\ 0 & 0 & e^{-j\xi_2} \end{bmatrix} \begin{bmatrix} \cos\gamma_2 & j\sin\gamma_2 & 0 \\ j\sin\gamma_2 & \cos\gamma_2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
&\qquad\left.\times \begin{bmatrix} e^{-j\xi_1}e^{2\pi j(-r_1/2R-s_1/2S)} & 0 & 0 \\ 0 & e^{2\pi j(r_1/2R+s_1/2S)} & 0 \\ 0 & 0 & e^{j\xi_1} \end{bmatrix}\right) \\
&= e^{j(\theta_1-\theta_2+\xi_1-\xi_2)}\det\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi j(-p_2/2P+q_2/2Q)} & 0 \\ 0 & 0 & e^{j(\theta_2+\xi_2)}e^{2\pi j(p_2/2P-q_2/2Q)} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma_1 & j\sin\gamma_1 \\ 0 & j\sin\gamma_1 & \cos\gamma_1 \end{bmatrix}\right. \\
&\qquad\times \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi j(p_1/2P-q_1/2Q)} & 0 \\ 0 & 0 & e^{-j(\theta_1+\xi_1)}e^{2\pi j(-p_1/2P+q_1/2Q)} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
&- \begin{bmatrix} e^{j(\theta_2+\xi_2)}e^{2\pi j((r_2/2R)+(s_2/2S))} & 0 & 0\\ 0 & e^{2\pi j(-(r_2/2R)-(s_2/2S))} & 0 \\ 0 & 0 & 1\end{bmatrix} \\
&\times \begin{bmatrix}\cos\gamma_2 & j\sin\gamma_2 & 0\\ j\sin\gamma_2 & \cos\gamma_2 & 0\\ 0 & 0 & 1\end{bmatrix} \begin{bmatrix} e^{-j(\theta_1+\xi_1)}e^{2\pi j(-r_1/2R-s_1/2S)} & 0 & 0\\ 0 & e^{2\pi j(r_1/2R+s_1/2S)} & 0\\ 0 & 0 & 1\end{bmatrix}\Bigg) = e^{j(\theta_1-\theta_2+\xi_1-\xi_2)} \\
\times \det &\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi j((p_1-p_2)/2P-(q_1-q_2)/2Q)}\cos\gamma_1 & je^{-j(\theta_1+\xi_1)}e^{2\pi j(-(p_1+p_2)/2P+(q_1+q_2)/2Q)}\sin\gamma_1 \\ 0 & je^{j(\theta_2+\xi_2)}e^{2\pi j((p_1+p_2)/2P-(q_1+q_2)/2Q)}\sin\gamma_1 & e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}e^{2\pi j(-(p_1-p_2)/2P+(q_1-q_2)/2Q)}\cos\gamma_1 \end{bmatrix} \right. \\
&\left. - \begin{bmatrix} e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}e^{2\pi j(-(r_1-r_2)/2R-(s_1-s_2)/2S)}\cos\gamma_2 & je^{j(\theta_2+\xi_2)}e^{2\pi j((r_1+r_2)/2R+(s_1+s_2)/2S)}\sin\gamma_2 & 0 \\ je^{-j(\theta_1+\xi_1)}e^{2\pi j(-(r_1+r_2)/2R-(s_1+s_2)/2S)}\sin\gamma_2 & e^{2\pi j((r_1-r_2)/2R+(s_1-s_2)/2S)}\cos\gamma_2 & 0 \\ 0 & 0 & 1\end{bmatrix}\right).
\end{aligned}
$$

$$
\begin{aligned}
y &= je^{2\pi j(-(p_1+p_2)/2P+(q_1+q_2)/2Q)}\sin 2\pi\left(\frac{p_1-p_2}{2P}+\frac{q_1-q_2}{2Q}\right) \text{ and} \\
z &= je^{2\pi j((r_1+r_2)/2R+(s_1+s_2)/2S)}\sin 2\pi\left(\frac{r_1-r_2}{2R}-\frac{s_1-s_2}{2S}\right). \\
\det(U_1-U_2) &= \bar{\Theta}\det\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & x & e^{-j(\theta_1+\xi_1)}y \\ 0 & -e^{j(\theta_2+\xi_2)}\bar{y} & e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}\bar{x}\end{bmatrix} - \begin{bmatrix} e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}w & e^{j(\theta_2+\xi_2)}z & 0 \\ -e^{-j(\theta_1+\xi_1)}\bar{z} & \bar{w} & 0 \\ 0 & 0 & 1\end{bmatrix}\right) \\
&= \bar{\Theta}\det\begin{bmatrix} 1-e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}w & -e^{j(\theta_2+\xi_2)}z & 0 \\ e^{-j(\theta_1+\xi_1)}\bar{z} & x-\bar{w} & e^{-j(\theta_1+\xi_1)}y \\ 0 & -e^{j(\theta_2+\xi_2)}\bar{y} & e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}\bar{x}-1\end{bmatrix} \\
&= \bar{\Theta}\left[(1-e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}w)(x-\bar{w})(e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}\bar{x}-1)\right. \\
&\qquad \left. + e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}|z|^2(e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}\bar{x}-1) + e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}|y|^2(1-e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}w)\right] \\
&= \bar{\Theta}\left[(1-\Theta w)(x-\bar{w})(\Theta\bar{x}-1)+\Theta|z|^2(\Theta\bar{x}-1)+\Theta|y|^2(1-\Theta w)\right] \\
&= \bar{\Theta}\left[(x-\Theta wx-\bar{w}+\Theta|w|^2)(\Theta\bar{x}-1)+\Theta|z|^2(\Theta\bar{x}-1)+\Theta|y|^2(1-\Theta w)\right] \\
&= \bar{\Theta}\left[(\Theta\bar{x}-1)(x-\Theta wx-\bar{w}+\Theta)+\Theta|y|^2(1-\Theta w)\right] \\
&= \bar{\Theta}\left[\Theta|x|^2-x-\Theta^2|x|^2w+\Theta wx-\Theta\bar{x}\bar{w}+\bar{w}+\Theta^2\bar{x}-\Theta+\Theta|y|^2-\Theta^2|y|^2w\right] \\
&= \bar{\Theta}\left[\Theta wx-\Theta\bar{x}\bar{w}-(x-\Theta^2\bar{x})-(\Theta^2w-\bar{w})\right] \\
&= wx-\bar{x}\bar{w}-(\bar{\Theta}x-\Theta\bar{x})-(\Theta w-\bar{\Theta}\bar{w}) = 2j(\mathcal{I}m(wx)-\mathcal{I}m\bar{\Theta}x-\mathcal{I}m\Theta w) \\
&= 2j\mathcal{I}m[(1-\bar{\Theta}x)(1-\Theta w)].
\end{aligned}
$$

Now, assume that P is even. Let us look at the two matrices U_1 and U_2 with $(q_1,r_1,s_1)=(q_2,r_2,s_2)$ and $p_1-p_2=P/2$. (Since P is even, this is achievable.) Therefore

$$
\begin{aligned}
&\det\left(U_1(p_1,q_1,r_1,s_1)-U_2(p_2,q_2,r_2,s_2)\right) \\
&\quad = 2j\mathcal{I}m\Bigg(\cos 2\pi\frac{p_1-p_2}{2P}e^{2\pi j(p_1-p_2)/2P} \\
&\qquad\qquad - \cos 2\pi\frac{p_1-p_2}{2P}e^{2\pi j(p_1-p_2)/2P}e^{2\pi j(p_1-p_2/P)} \\
&\qquad\qquad - e^{2\pi j(-(p_1-p_2)/P)}\Bigg) \\
&\quad = 2j\left(\cos\frac{\pi}{2}\sin\frac{\pi}{2}-\cos\frac{\pi}{2}\sin\frac{3\pi}{2}-\sin(-\pi)\right) \\
&\quad = 0.
\end{aligned}
$$

$\mathcal{C}^{(1)}$ is not fully diverse. By a similar argument, when Q, R, or S is even, $\mathcal{C}^{(1)}$ is not fully diverse. □

APPENDIX D
PROOF OF THEOREM 5

Proof: Define $\theta_i = 2\pi(\pm p_i/P \pm q_i/Q)$ and $\xi_i = 2\pi(\pm r_i/R \pm s_i/S)$ for $i=1,2$. For any $U_1(p_1,q_1,r_1,s_1)$ and $U_2(p_2,q_2,r_2,s_2)$ in $\mathcal{C}^{(2)}$, $U_1 = A^{(2)}_{(p_1,q_1)}B^{(2)}_{(r_1,s_1)}$ and $U_2 = A^{(2)}_{(p_2,q_2)}B^{(2)}_{(r_2,s_2)}$, where $A^{(2)}$ and $B^{(2)}$ are as defined in (14). By a similar argument in the proof of Theorem 2, we have the second equation on the top of this page. Therefore, we have the equation at the top of the next page. □

$$
\begin{aligned}
&\det(U_1(p_1,q_1,r_1,s_1)-U_2(p_2,q_2,r_2,s_2)=\det A^{(2)}_{(p_2,q_2)}\det B^{(2)}_{(r_1,s_1)}\det\left(\left(A^{(2)}_{(p_2,q_2)}\right)^{-1}A^{(2)}_{(p_1,q_1)}-B^{(2)}_{(r_2,s_2)}\left(B^{(2)}_{(r_1,s_1)}\right)^{-1}\right)\\
&=e^{j\theta_1}e^{-j\xi_2}\det\left(\begin{bmatrix}1&0&0\\0&x&e^{-j\xi_1}y\\0&-e^{j\xi_2}\bar{y}&e^{-j(\xi_1-\xi_2)}\bar{x}\end{bmatrix}-\begin{bmatrix}e^{-j(\theta_1-\theta_2)}w&e^{j\theta_2}z&0\\-e^{-j\theta_1}\bar{z}&\bar{w}&0\\0&0&1\end{bmatrix}\right)\\
&=e^{j\theta_1}e^{-j\xi_2}\det\begin{bmatrix}1-e^{-j(\theta_1-\theta_2)}w&-e^{j\theta_2}z&0\\e^{-j\theta_1}\bar{z}&x-\bar{w}&e^{-j\xi_1}y\\0&-e^{j\xi_2}\bar{y}&e^{-j(\xi_1-\xi_2)}\bar{x}-1\end{bmatrix}\\
&=e^{j\theta_1}e^{-j\xi_2}\left[(e^{-j(\xi_1-\xi_2)}-e^{-j(\theta_1-\theta_2)})-(x-e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}\bar{x})+(\bar{w}-e^{-j(\theta_1-\theta_2+\xi_1-\xi_2)}w)+(e^{-j(\theta_1-\theta_2)}wx-e^{-j(\xi_1-\xi_2)}\bar{x}\bar{w})\right]\\
&=e^{j\theta_1}e^{-j\xi_2}\left[\left(\bar{\Theta}_2^2-\bar{\Theta}_1^2\right)-\left(x-\bar{\Theta}_1^2\bar{\Theta}_2^2\bar{x}\right)+\left(\bar{w}-\bar{\Theta}_1^2\bar{\Theta}_2^2w\right)+\left(\bar{\Theta}_1^2wx-\bar{\Theta}_2^2\bar{x}\bar{w}\right)\right]\\
&=e^{j\theta_1}e^{-j\xi_2}\bar{\Theta}_1\bar{\Theta}_2\left[(\Theta_1\bar{\Theta}_2-\overline{\Theta_1\bar{\Theta}_2})-(\Theta_1\Theta_2x-\overline{\Theta_1\Theta_2x})-(\bar{\Theta}_1\bar{\Theta}_2w-\overline{\bar{\Theta}_1\bar{\Theta}_2w})+(\bar{\Theta}_1\Theta_2wx-\overline{\bar{\Theta}_1\Theta_2wx})\right]\\
&=2je^{j\theta_1}e^{-j\xi_2}\bar{\Theta}_1\bar{\Theta}_2\mathcal{I}m(\Theta_1\bar{\Theta}_2-\Theta_1\Theta_2x-\bar{\Theta}_1\bar{\Theta}_2w+\bar{\Theta}_1\Theta_2wx)\\
&=2je^{j\theta_1}e^{-j\xi_2}\bar{\Theta}_1\bar{\Theta}_2\mathcal{I}m[(\Theta_1-\bar{\Theta}_1w)(\bar{\Theta}_2-\Theta_2x)]\\
&=2je^{j\theta_1}e^{-j\xi_2}\bar{\Theta}_1\bar{\Theta}_2\mathcal{I}m\left[\Theta_1\bar{\Theta}_2\left(1-\bar{\Theta}_1^2w\right)\left(1-\Theta_2^2x\right)\right].
\end{aligned}
$$

APPENDIX E
PROOF OF THEOREM 6

Proof: For code $\mathcal{C}^{(2)}$ to be fully diverse, $\left\{A^{(2)}_{(p,q)}\right\}$ and $\left\{B^{(2)}_{(r,s)}\right\}$ must be fully diverse. Therefore, from Theorem 4, $\gcd(P,Q)=\gcd(R,S)=1$ are necessary conditions.

Assume that both P and R are even. For any two matrices $U_1(p_1,q_1,r_1,s_1)$ and $U_2(p_2,q_2,r_2,s_2)$ in $\mathcal{C}^{(2)}$, choose $q_1=q_2$, $s_1=s_2$, $p_1-p_2=P/2$, and $r_1-r_2=R/2$. Since both P and R are even, this is achievable, and the two matrices are different. Therefore, from the proof of Theorem 2

$$
\begin{aligned}
&|\det(U_1(p_1,q_1,r_1,s_1)-U_2(p_2,q_2,r_2,s_2))|\\
&\quad=2\left|\mathcal{I}m(\Theta_1\bar{\Theta}_2-\Theta_1\Theta_2x-\bar{\Theta}_1\bar{\Theta}_2w+\bar{\Theta}_1\Theta_2wx)\right|
\end{aligned}
$$

where

$$
\begin{aligned}
x&=e^{2\pi j((p_1-p_2)/2P-(q_1-q_2)/2Q)}\\
&\quad\times\cos 2\pi\left(\frac{p_1-p_2}{2P}+\frac{q_1-q_2}{2Q}\right)\\
&=e^{j(\pi/2)}\cos\frac{\pi}{2}=0\\
w&=e^{2\pi j(-(r_1-r_2)/2R-(s_1-s_2)/2S)}\\
&\quad\times\cos 2\pi\left(\frac{r_1-r_2}{2R}-\frac{s_1-s_2}{2S}\right)\\
&=e^{-j(\pi/2)}\cos\frac{\pi}{2}=0\\
\Theta_1&=e^{2\pi j(\pm(p_1-p_2)/2P\pm(q_1-q_2)/2Q)}=e^{\pm j(\pi/2)},\text{ and}\\
\Theta_2&=e^{2\pi j(\pm(r_1-r_2)/2R\pm(s_1-s_2)/2S)}=e^{\pm j(\pi/2)}.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
&|\det(U_1(p_1,q_1,r_1,s_1)-U_2(p_2,q_2,r_2,s_2))|\\
&\qquad\qquad=2\left|\mathcal{I}m(\Theta_1\bar{\Theta}_2)\right|=0
\end{aligned}
$$

which indicates that the code is not fully diverse. By a similar argument, we can prove that when any two of the integers $\{P,Q,R,S\}$ are even, $\mathcal{C}^{(2)}$ is not fully diverse. Therefore, a necessary condition for $\mathcal{C}^{(2)}$ to be fully diverse is $\gcd(P,Q)=\gcd(R,S)=1$, and among the four integers $\{P,Q,R,S\}$, at most one is even.

What is left is to prove that for the type I AB code, we need $\gcd(P,R)=\gcd(P,S)=\gcd(Q,R)=\gcd(Q,S)=1$. We prove this by contradiction. Assume that $\gcd(P,R)=G>1$. Let $p_1=p_2+G$, $q_1=q_2$, $r_1=r_2+G$, and $s_1=s_2$. We have $\Theta_1=\Theta_2=e^{-j(2\pi/G)}$ and $x=\bar{w}=e^{j(\pi/G)}\cos(\pi/G)$. It is easy to check by (18) that $\det(U_1-U_2)=0$. Therefore, $\gcd(P,R)=1$ is a necessary condition. The same is true for other pairs. □

REFERENCES

[1] B. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2041–2052, Dec. 2000.

[2] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *J. Sel. Areas Commun.*, vol. 18, no. 7, pp. 1169–1174, Jul. 2000.

[3] B. Hughes, "Differential space-time modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2567–2578, Nov. 2000.

[4] A. Shokrollahi, B. Hassibi, B. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2335–2367, Sep. 2001.

[5] B. Hughes, "Optimal space-time constellations from groups," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 401–410, Feb. 2000.

[6] B. Hassibi and M. Khorrami, "Fully-diverse multiantenna constellations and fixed-point-free Lie groups," in *Proc. Int. Symp. Inf. Theory*, Jun. 2001, p. 199.

[7] A. Shokrollahi, Design of Unitary Space-Time Codes From Representations of $SU(2)$, 2000, to be published.

[8] Y. Jing and B. Hassibi, "Design of fully diverse multiple-antenna codes based on Sp(2)," *IEEE Trans. Inf. Theory*, no. 11, pp. 2639–2656, Nov. 2004.

[9] S. M. Alamouti, "A simple transmitter diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[10] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat-fading," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 139–157, Jan. 1999.

[11] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–564, Mar. 2000.

[12] B. Hassibi and B. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1458–1503, Jun. 2002.

[13] B. Simon, *Representations of Finite and Compact Lie Groups*. Providence, RI: Amer. Math. Soc., 1994.

[14] A. Song, G. Wang, W. Wu, and X.-G. Xia, "Unitary space-time codes from Alamouti's scheme with APSK signals," *IEEE Trans. Wireless Communications*, vol. 3, no. 6, pp. 2374–2384, Sep. 2004.

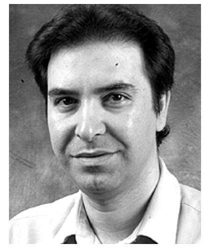
[15] B. Hochwald and S. ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 389–399, Mar. 2003.

[16] M. O. Damen, K. Abed-Meraim, and M. S. Lemdani, "Further results on the sphere decoder algorithm," *IEEE Trans. Inf. Theory*, submitted for publication.

[17] B. Hassibi and H. Vikalo, "On the expected complexity of integer least-squares problems," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Apr. 2002, pp. 1497–1500.

Yindi Jing received the B.S. and M.S. degrees in automatic control from the University of Science and Technology of China, Hefei, in 1996 and 1999. She received another M.S. degree as well as the Ph.D. degree in electrical engineering from the California Institute of Technology, Pasadena, in 2000 and 2004, respectively, where she is currently a postdoctoral scholar.

Her research interests are in the areas of wireless communications and signal processing, especially the theoretical analysis and unitary space-time code design of multiple-antenna wireless communication systems, with emphasis on random matrix theory and group representation theory. She is also working on the analysis, design, and signal processing in *ad hoc* wireless networks.



Babak Hassibi was born in Tehran, Iran, in 1967. He received the B.S. degree from the University of Tehran in 1989 and the M.S. and Ph.D. degrees from Stanford University, Stanford, CA, in 1993 and 1996, respectively, all in electrical engineering.

From October 1996 to October 1998, he was a research associate with the Information Systems Laboratory, Stanford University, and from November 1998 to December 2000, he was a Member of the Technical Staff with the Mathematical Sciences Research Center, Bell Laboratories, Murray Hill, NJ. Since January 2001, he has been an assistant professor of electrical engineering at the California Institute of Technology, Pasadena. He has also held short-term appointments at Ricoh California Research Center, Menlo Park, CA, the Indian Institute of Science, Bangalore, India, and Linköping University, Linköping, Sweden. His research interests include wireless communications, robust estimation and control, adaptive signal processing and linear algebra. He is the coauthor of the books *Indefinite Quadratic Estimation and Control: A Unified Approach to H^2 and H^∞ Theories* (New York: SIAM, 1999) and *Linear Estimation* (Englewood Cliffs, NJ: Prentice-Hall, 2000). He is a recipient of the Alborz Foundation Fellowship, the 1999 Hugo Schuck Best Paper Award of the American Automatic Control Council, the 2002 National Science Foundation Career Award, the 2002 Okawa Foundation Research Grant for Information and Telecommunications, the 2003 David and Lucille Packard Fellowship for Science and Engineering, and the 2003 Presidential Early Career Award for Scientists and Engineers (PECASE). He was a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY Special Issue on "Space-Time Transmission, Reception, Coding, and Signal Processing" and is currently an Associate Editor Communications for the IEEE TRANSACTIONS ON INFORMATION THEORY.